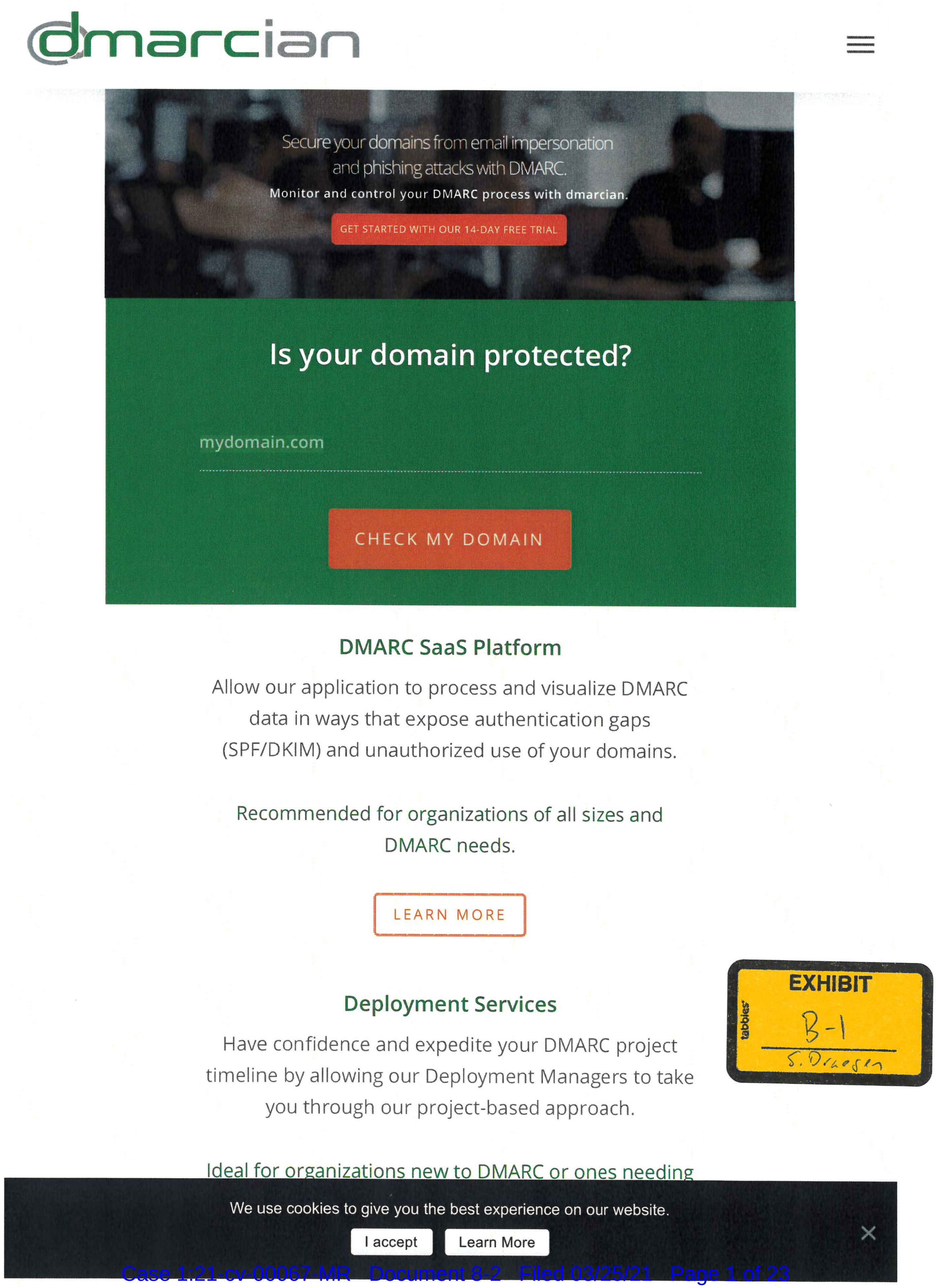


Secure your domains from email impersonation and phishing attacks with DMARC.

Monitor and control your DMARC process with dmarcian.

Is your domain protected?

DMARC SaaS Platform

Allow our application to process and visualize DMARC data in ways that expose authentication gaps (SPF/DKIM) and unauthorized use of your domains.

Recommended for organizations of all sizes and DMARC needs.

Deployment Services

Have confidence and expedite your DMARC project timeline by allowing our Deployment Managers to take you through our project-based approach.

Ideal for organizations new to DMARC or ones needing

We use cookies to give you the best experience on our website.

EXHIBIT
tabbies
B-1
S. Draegen

DMARC alignment

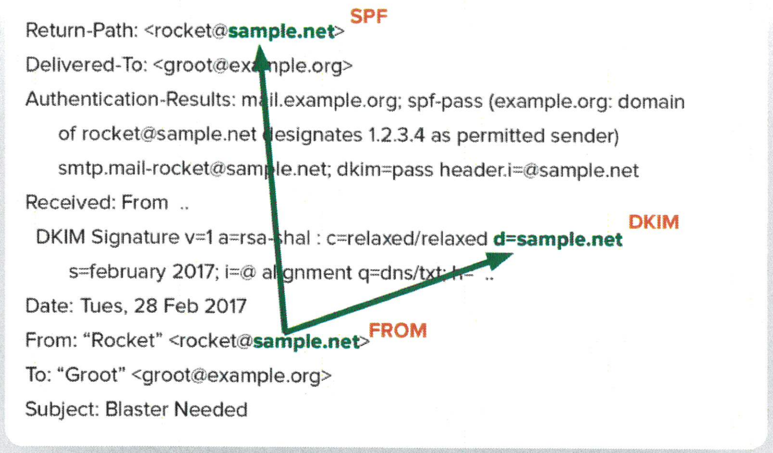
By themselves, SPF and DKIM can associate a piece of email with a domain. DMARC attempts to tie the results of SPF and DKIM to the content of email, specifically to the domain found in the From: header of an email. The domain found in the From: header of a piece of email is the entity that ties together all DMARC processing.

Because anyone can buy a domain and put SPF and DKIM into place (including criminals), the results of processing SPF and DKIM have to be related to the domain found in the From: header to be relevant to DMARC. This concept is referred to as Identifier Alignment.

Identifier Alignment is how existing email authentication technologies are made relevant to the content of an email. Getting identifiers to align ends up being a large part of the work of deploying DMARC.

Are your SPF and DKIM identifiers aligned?

When your email is sent, the “From domain” has your domain name after the @ within the email address. Your DKIM signature should also contain the same domain name embedded into the key string. If they



```
Return-Path: <rocket@sample.net>
Delivered-To: <groot@example.org>
Authentication-Results: mail.example.org; spf-pass (example.org: domain
    of rocket@sample.net designates 1.2.3.4 as permitted sender)
    smtp.mail-rocket@sample.net; dkim=pass header.i=@sample.net
Received: From  ..
  DKIM Signature v=1 a=rsa-sha1 : c=relaxed/relaxed d=sample.net
      s=february 2017; i=@ alignment q=dns/txt; h=  ..
Date: Tues, 28 Feb 2017
From: “Rocket” <rocket@sample.net>
To: “Groot” <groot@example.org>
Subject: Blaster Needed
```

Configuring third-party sources

Third-party sources (eg. SendGrid, Amazon SES, Salesforce, etc.) often use their domain name space to get SPF and DKIM to pass. Configuring these third-party sources to use your own domain name space will bring about alignment. Each third-party source has varying capabilities in this area. dmarcian has cataloged and detailed over 900 third-party sources, their capabilities, and instructions on how to configure related settings.

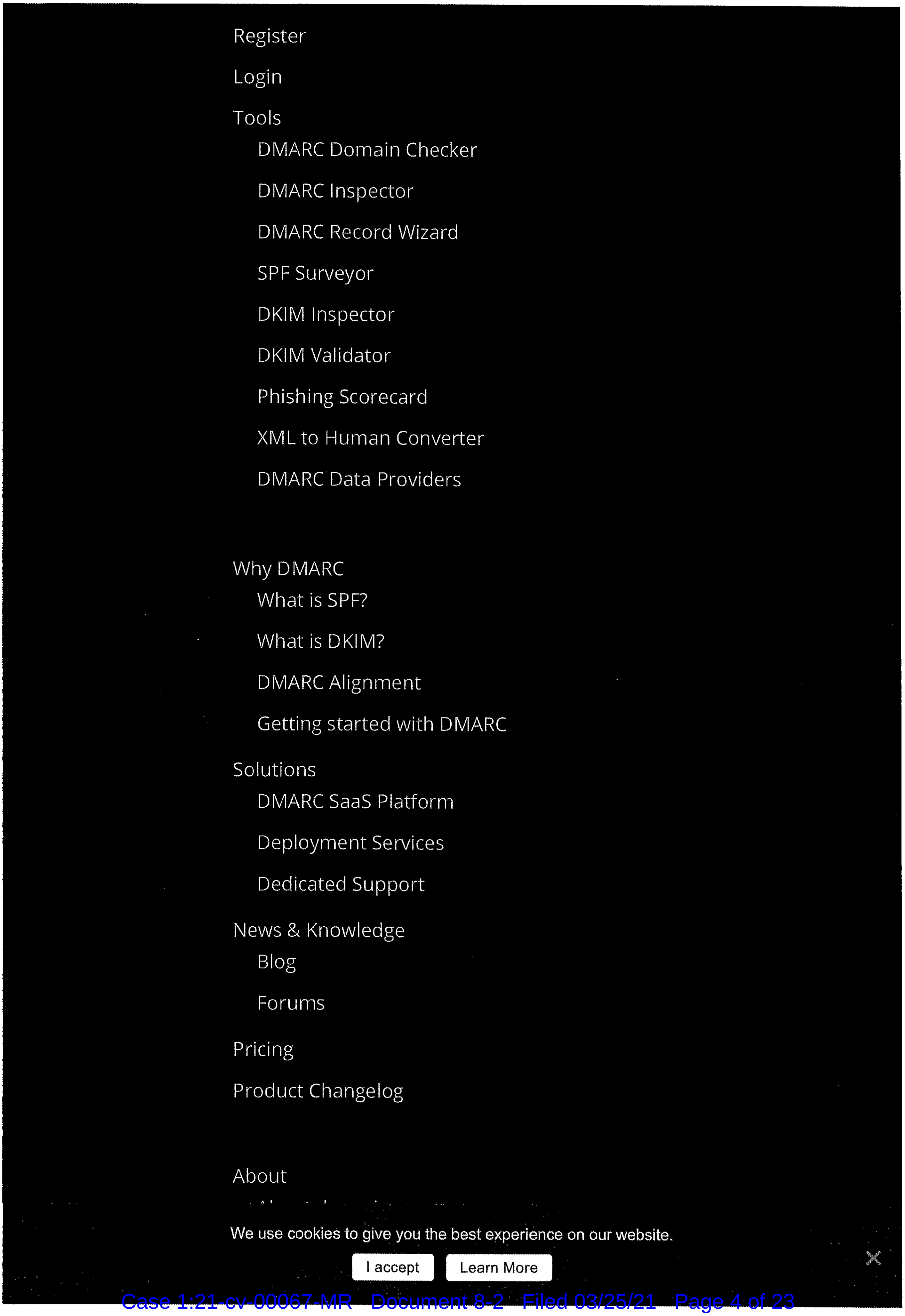
Get your domains into compliance. Try out dmarcian for free!

SIGN UP FREE

CONTACT US

We use cookies to give you the best experience on our website.

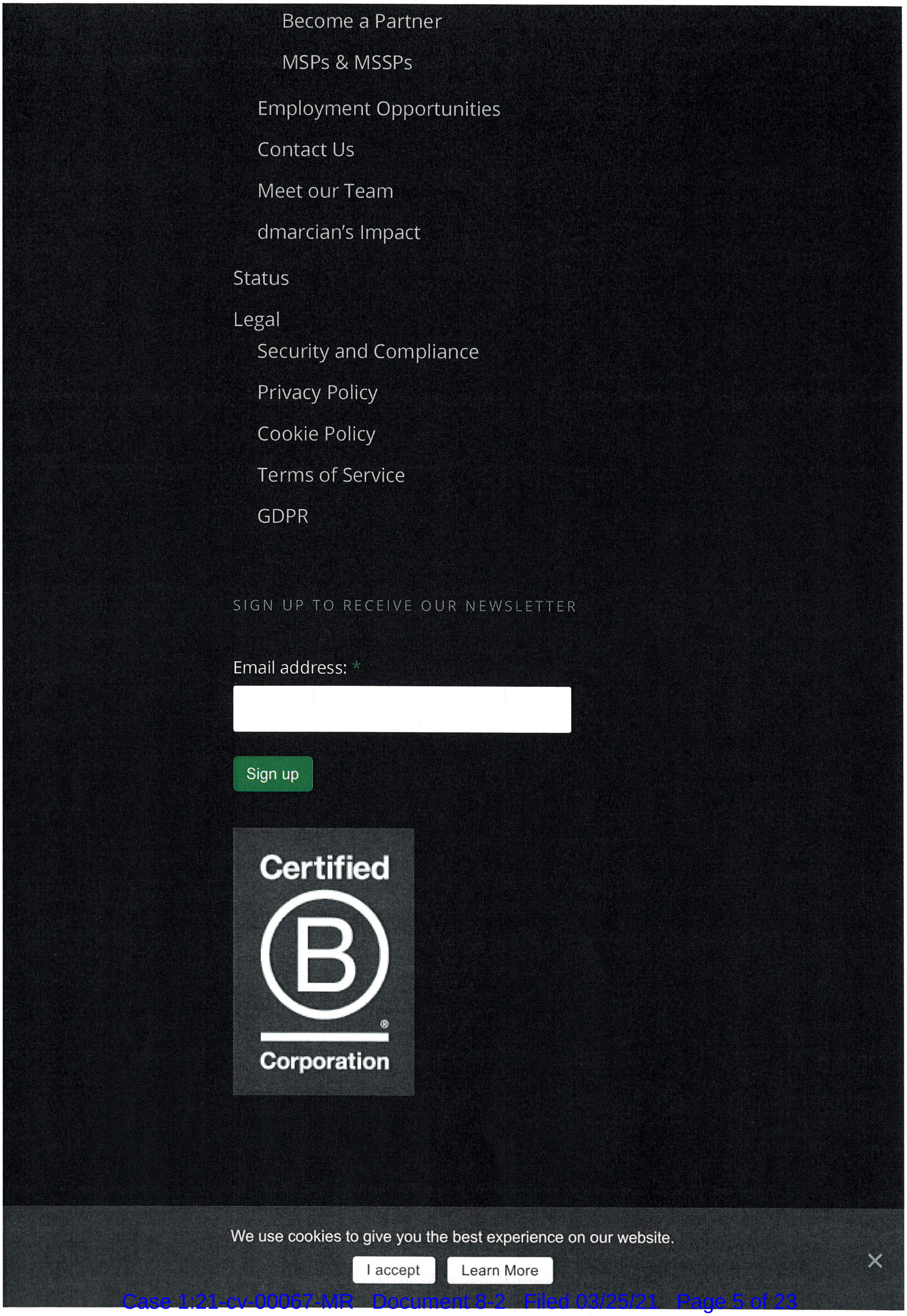
I accept Learn More ×



- Register
- Login
- Tools
  - DMARC Domain Checker
  - DMARC Inspector
  - DMARC Record Wizard
  - SPF Surveyor
  - DKIM Inspector
  - DKIM Validator
  - Phishing Scorecard
  - XML to Human Converter
  - DMARC Data Providers
- Why DMARC
  - What is SPF?
  - What is DKIM?
  - DMARC Alignment
  - Getting started with DMARC
- Solutions
  - DMARC SaaS Platform
  - Deployment Services
  - Dedicated Support
- News & Knowledge
  - Blog
  - Forums
- Pricing
- Product Changelog
- About

We use cookies to give you the best experience on our website.

I accept Learn More ×



Become a Partner

MSPs & MSSPs

Employment Opportunities

Contact Us

Meet our Team

dmarcian’s Impact

Status

Legal

Security and Compliance

Privacy Policy

Cookie Policy

Terms of Service

GDPR

SIGN UP TO RECEIVE OUR NEWSLETTER

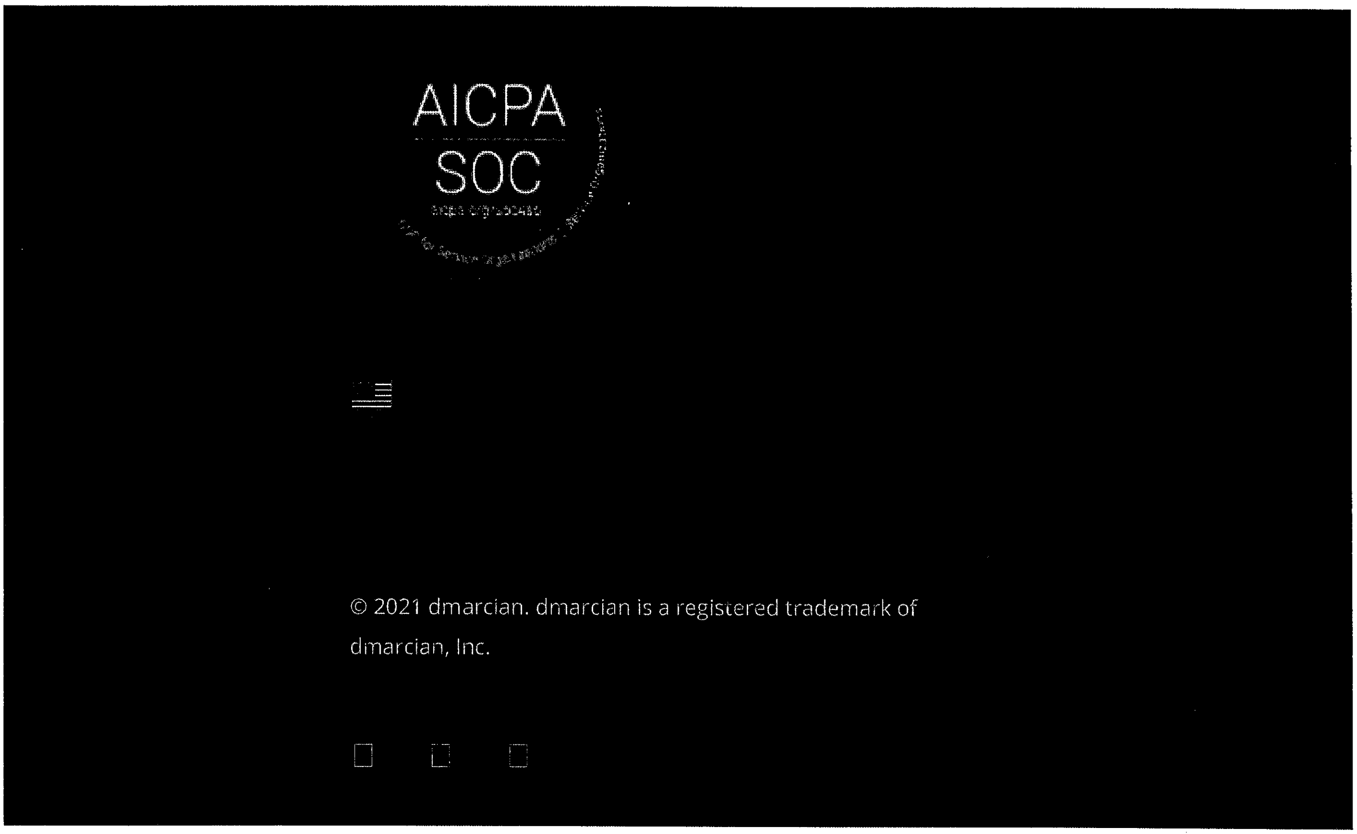
Email address: *

Sign up

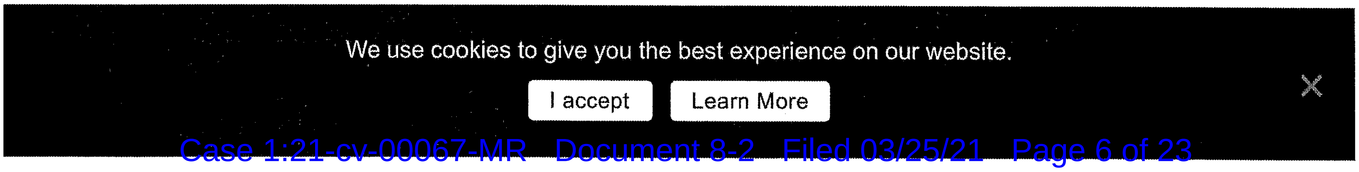
Certified B Corporation

We use cookies to give you the best experience on our website.

I accept Learn More ✕



© 2021 dmarcian. dmarcian is a registered trademark of dmarcian, Inc.



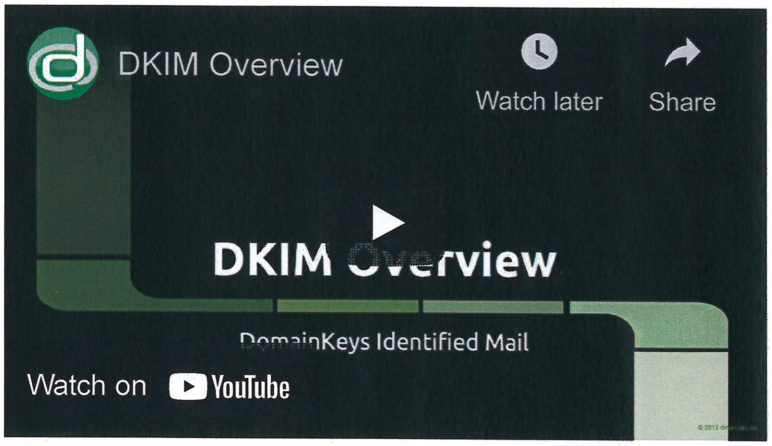
We use cookies to give you the best experience on our website.

What is DKIM?

DKIM Explained

DKIM stands for **D**omain**K**eys **I**dentified **M**ail and is used for the authentication of an email that's being sent. Like SPF, DKIM is an open standard for email authentication that is used for DMARC alignment. A DKIM record exists in the DNS, but it is a bit more complicated than SPF. DKIM's advantage is that it can survive forwarding, which makes it superior to SPF and a foundation for securing your email.

Starting in 2004 from merging two similar efforts, "enhanced DomainKeys" from Yahoo and "Identified Internet Mail" from Cisco and has since been widely adopted for email authentication.



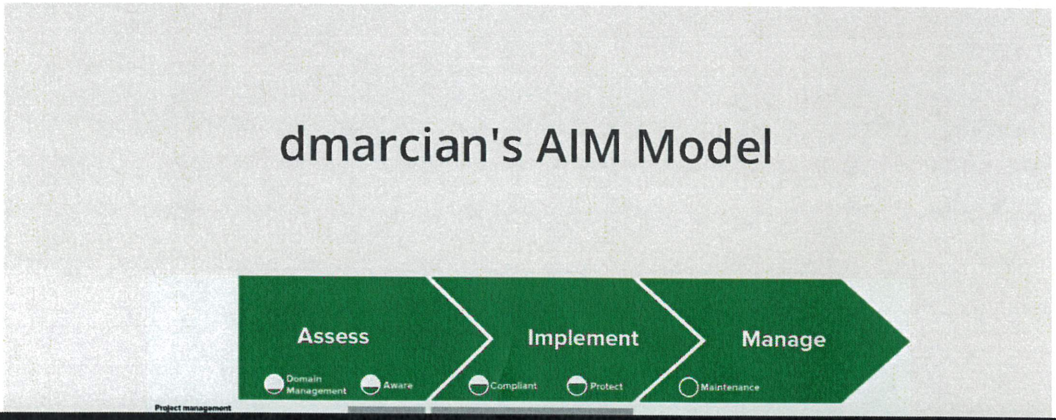
What is a DKIM Record?

A domain owner adds a DKIM record, which is a modified TXT record, to the DNS records on the sending

Deployment Services

dmarcian Deployment Services are project-based initiatives that help you achieve your DMARC objectives and milestones. Each project maintains the necessary education, training and policy enactments to ensure you can be self-sufficient in managing your domain catalog and email footprint when the project comes to conclusion.

Deployment projects commence with education and training modules to ensure you understand the entirety of the program scope and can take action with the appropriate context. Subsequent sessions will take the form of weekly meetings championed by the Deployment Manager. Most sessions will include a screen-share meeting room, option to record, and leave-behind assets.



dmarcian's AIM Model

Over the last six years, **dmarcian** has developed a project-based approach—our AIM model—for policy enforcement that addresses technical compliance and how it affects different aspects of your organization.

Phase 1: Assess

The Assess phase starts with gathering your organizational domains and collecting data about them using the DMARC policy of *p=none*. Then we'll perform an impact analysis on the results in order to categorize the domains and create an accurate implementation plan.

Phase 2: Implement

The Implement phase focuses on enabling email authentication based on the plan created during the Assess stage. The goal here is to make each email source DMARC compliant by deploying SPF and DKIM technologies. Once an agreed-upon coverage is reached, we'll move away from monitoring mode to a *p=reject* DMARC policy.

Phase 3: Manage

The last phase of the project is focused on preparing your organization for the future on two main fronts: unexpected problems and planned changes. We'll enable reports and alerts for cases when we see infrastructure hurdles. Most importantly, we'll establish a new business process for onboarding new digital assets.

We use cookies to give you the best experience on our website.

I accept Learn More ×

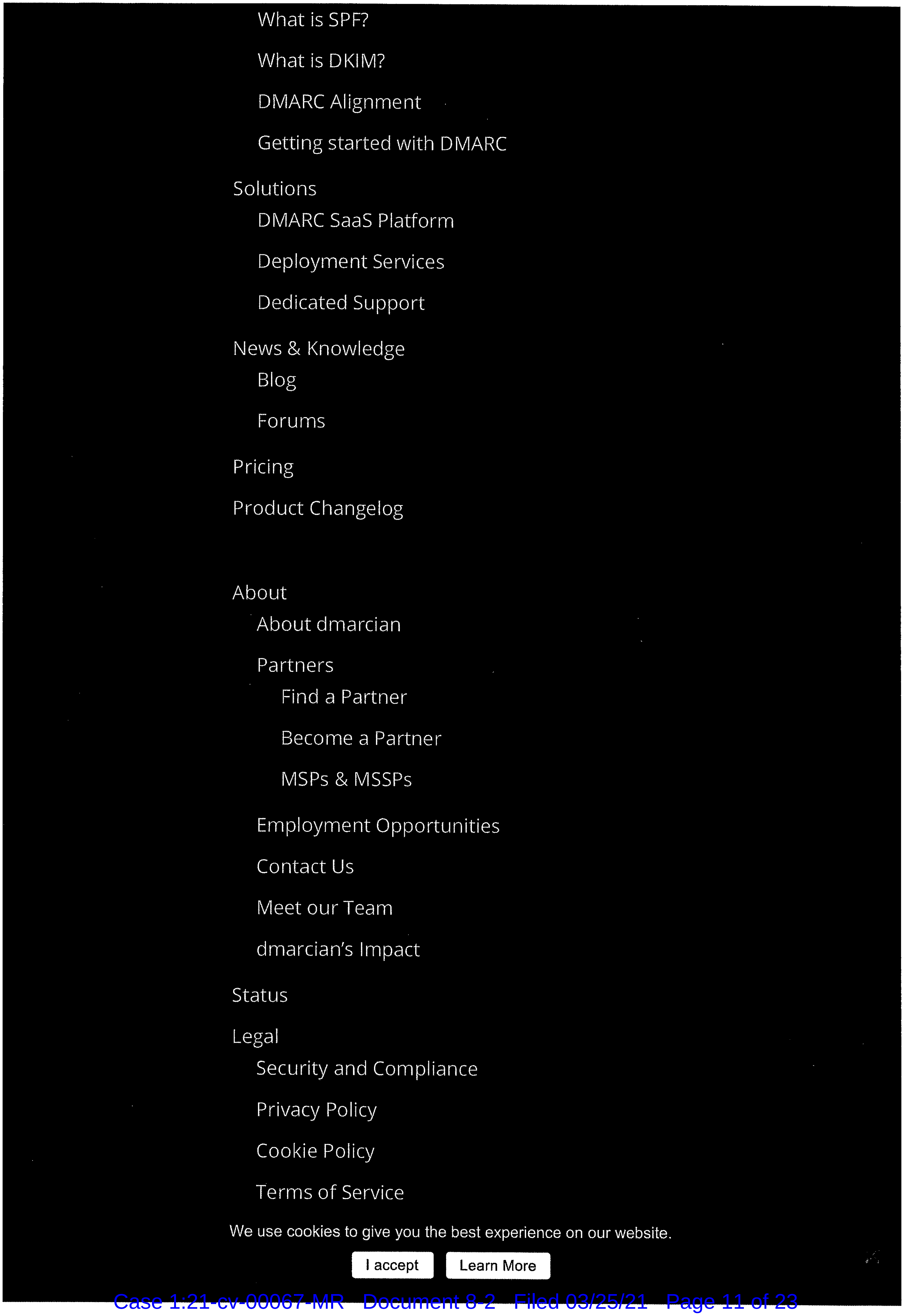
dmarcian was founded by one of DMARC's primary authors, and we have an international track record for helping businesses and governmental organizations across the globe and of all sizes successfully deploy DMARC. We can tailor to the needs of your organization, from light-touch initial onboarding through full outsourcing of all DMARC-related functions and monitoring. Contact us to get started.

Get your domains into compliance. Try out dmarcian for free!

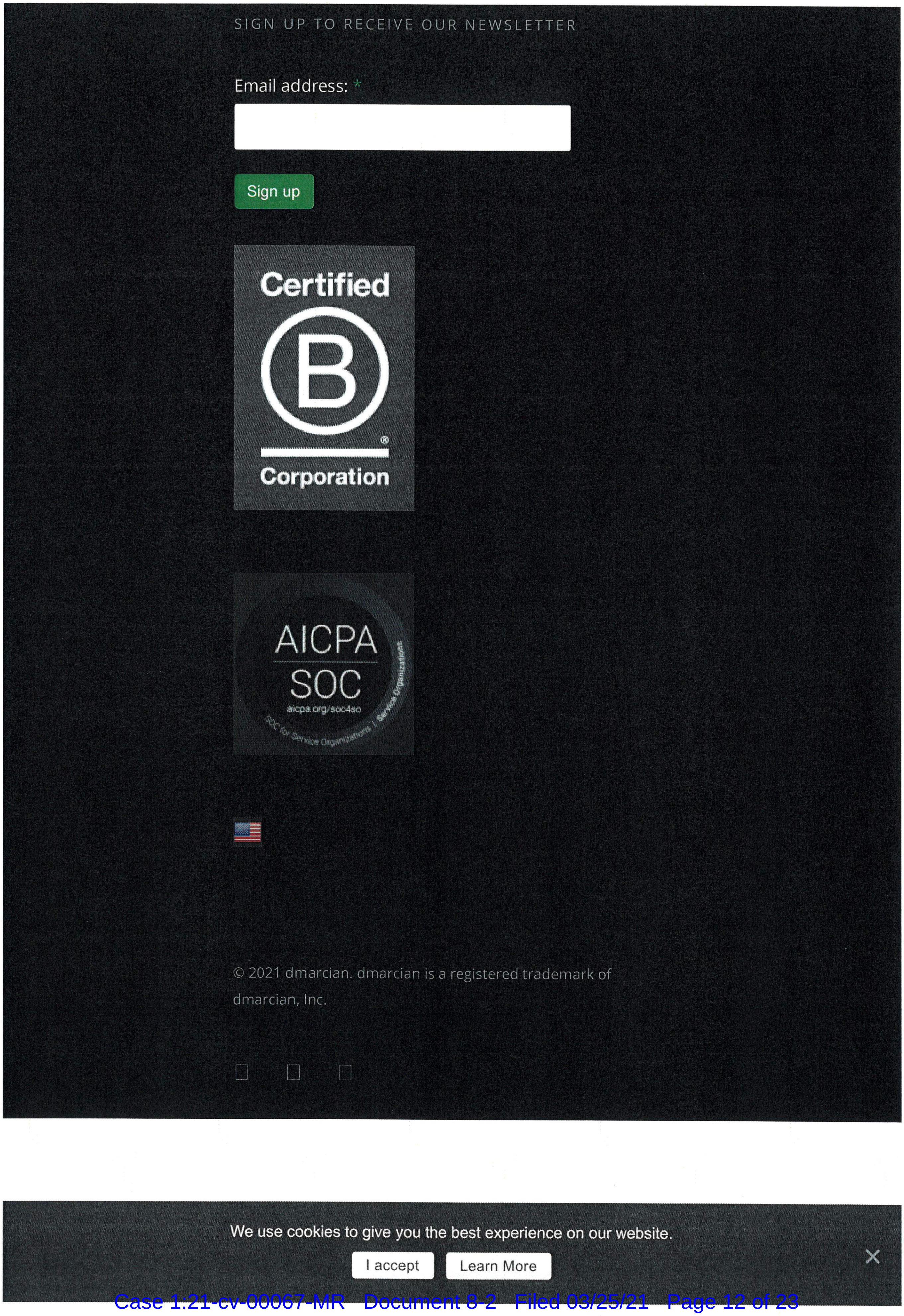
SIGN UP FREE

CONTACT US

- Register
- Login
- Tools
  - DMARC Domain Checker
  - DMARC Inspector
  - DMARC Record Wizard
  - SPF Surveyor
  - DKIM Inspector
  - DKIM Validator
  - Phishing Scorecard
  - XML to Human Converter
  - DMARC Data Providers



We use cookies to give you the best experience on our website.



SIGN UP TO RECEIVE OUR NEWSLETTER

Email address: *

© 2021 dmarcian. dmarcian is a registered trademark of dmarcian, Inc.

We use cookies to give you the best experience on our website.

dmarcian

DMARC SaaS Platform

dmarcian's DMARC SaaS platform receives, processes and classifies mail observed from your domain namespace and makes sense of it for you. The native XML format in which DMARC data is transmitted is not intended for human consumption. Our platform visualizes the data in powerful and meaningful ways so you can quickly identify authentication gaps (SPF/DKIM) and unauthorized use of your domains.

In addition to aggregating DMARC data, our platform provides domain administration teams with the necessary features to adopt DMARC with clarity and confidence. The dmarcian reporting platform sits atop the most accurate source classification engine in the industry and affords users with assurances of the true origin of a particular mail stream.

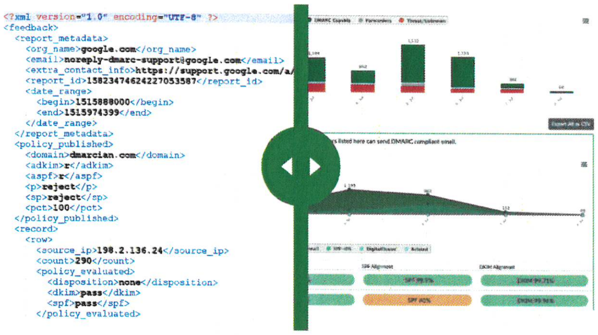
dmarcian has been processing DMARC data since the inception of the specification in 2012.

We use cookies to give you the best experience on our website.

I accept Learn More

Without dmarcian

This—times a whole lot more, depending on the amount of email you send.



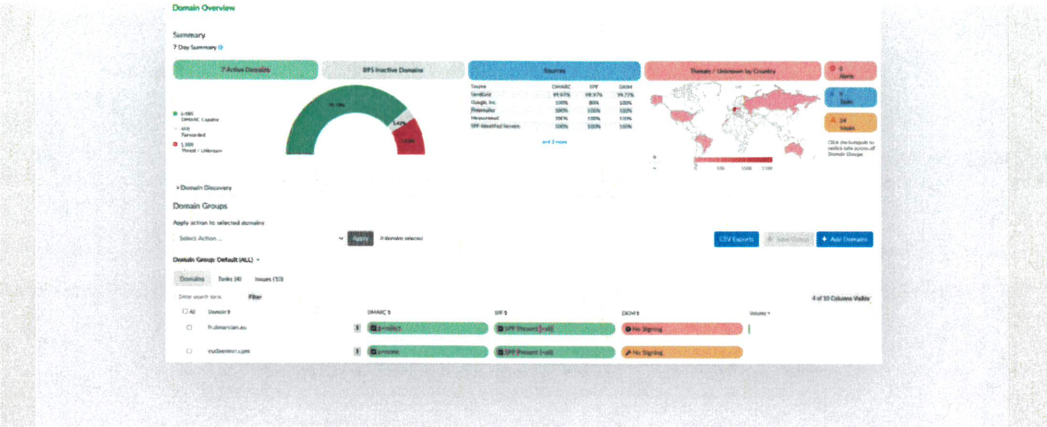
```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/
    <report_id>15823474624227053587</report_id>
    <date_range>
      <begin>1515888000</begin>
      <end>1515974399</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>dmarcian.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>198.2.136.24</source_ip>
      <count>290</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
```

With dmarcian

DMARC's XML feedback contains useful information, and **dmarcian** helps you make sense of it.

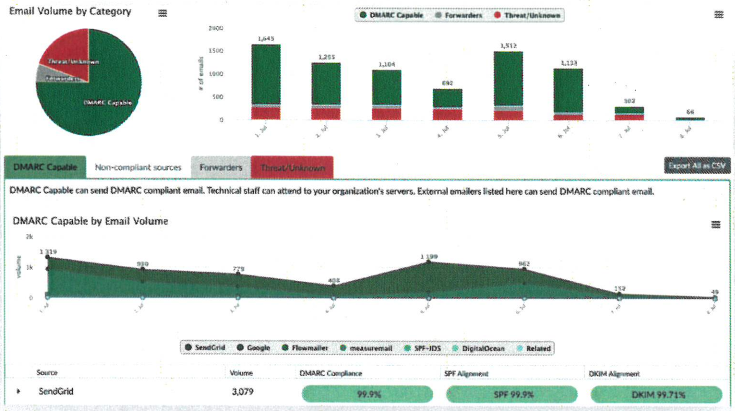
Domain Overview

The Domain Overview contains a summary of the status of all your domains and sources. The geographical location of recent abuse is also shown. View the state of your domains at a glance, and get to work locking down your email domains.



Detail Viewer

The Detail Viewer allows you to explore your DMARC data in a variety of ways. It shows a timeline of your data along with search parameters such as From and To date selectors, domain and data-provider pickers, and a filter option that can be used to show what would have happened had a DMARC policy been in place.



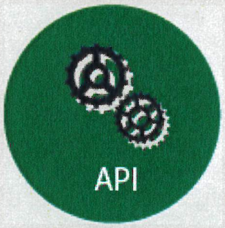
DMARC Capable can send DMARC compliant email. Technical staff can attend to your organization's servers. External emailers listed here can send DMARC compliant email.

Source	Volume	DMARC Compliance	SPF Alignment	DKIM Alignment
▸ SendGrid	3,079	99.9%	SPF 99.9%	DKIM 99.71%

The Detail Viewer also shows your data grouped into four high-level tabs: DMARC-capable, Non-compliant, Forwarding, and Threat/Unknown. Each tab shows groups of infrastructure and details on DMARC compliance. You can find more information on how to get DMARC compliant per source. You can reveal more detail about each group and discover the sources of your domain's email and combine data from multiple providers across specific

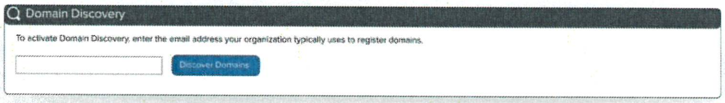
API

Integrate our DMARC SaaS Platform seamlessly into your own dashboards or SOC by using our API. This is an Enterprise plan only feature.



Domain Discovery

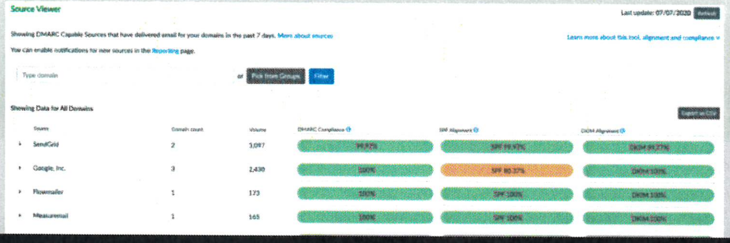
Not sure what domains you have registered? **dmarcian** can help. Using Domain Discovery, dmarcian can automatically discover your digital assets and add them to your catalogue. This is an Enterprise plan only feature.



To activate Domain Discovery, enter the email address your organization typically uses to register domains.

Source Viewer

The Source Viewer shows an overview of the DMARC Capable Sources we have found across all of your domains or domain groups.



Last update: 07/07/2020

Showing DMARC Capable Sources that have delivered email for your domains in the past 7 days. More about sources

Learn more about this tool, alignment and compliance

You can enable notifications for new sources in the Reporting page.

Showing Data for All Domains

Source	Domain count	Volume	DMARC Compliance	SPF Alignment	DKIM Alignment
SendGrid	2	3,097	99.93%	SPF 99.93%	DKIM 99.27%
Google, Inc.	3	2,430	100%	SPF 80.37%	DKIM 100%
Flowmailer	1	173	100%	SPF 100%	DKIM 100%
Measuremail	1	165	100%	SPF 100%	DKIM 100%

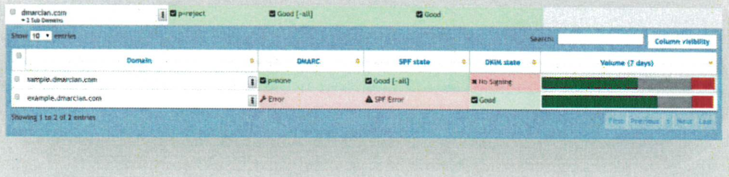
Single Sign-On

Our DMARC SaaS Platform allows our customers to extend their security setup using Single Sign-On. Single Sign-On lets organizations define/manage access requirements and simplifies provisioning and deprovisioning of users. We currently support SAML V2.0. This is an Enterprise-only feature.

Single Sign-On

Automatic Subdomain Detection

Our DMARC SaaS Platform automatically detects, processes, sorts and displays subdomains and gives users the option to choose which subdomains are valuable to them.



□ dmarcian.com ▾ 2 Sub Domains	☑ p=reject	☑ Good [-all]	☑ Good	

Show 10 ▾ entries

Search:

□ Domain	DMARC	SPF state	DKIM state	Volume (7 days)
□ sample.dmarcian.com	☑ p=none	☑ Good [-all]	☒ No Signing	
□ example.dmarcian.com	Error	⚠ SPF Error	☑ Good	

Showing 1 to 2 of 2 entries

Get your domains into compliance. Try out dmarcian for free!

SIGN UP FREE

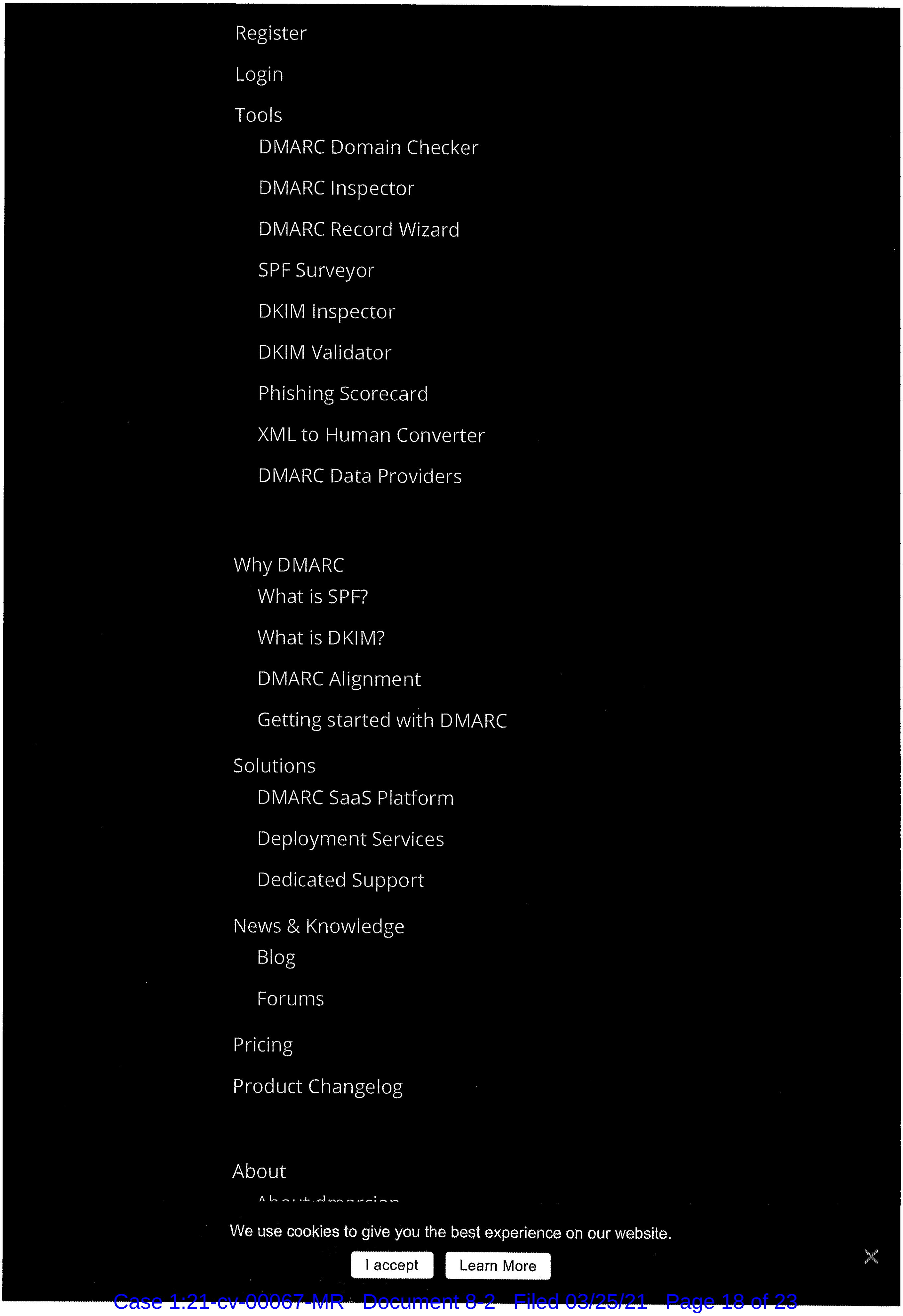
CONTACT US

We use cookies to give you the best experience on our website.

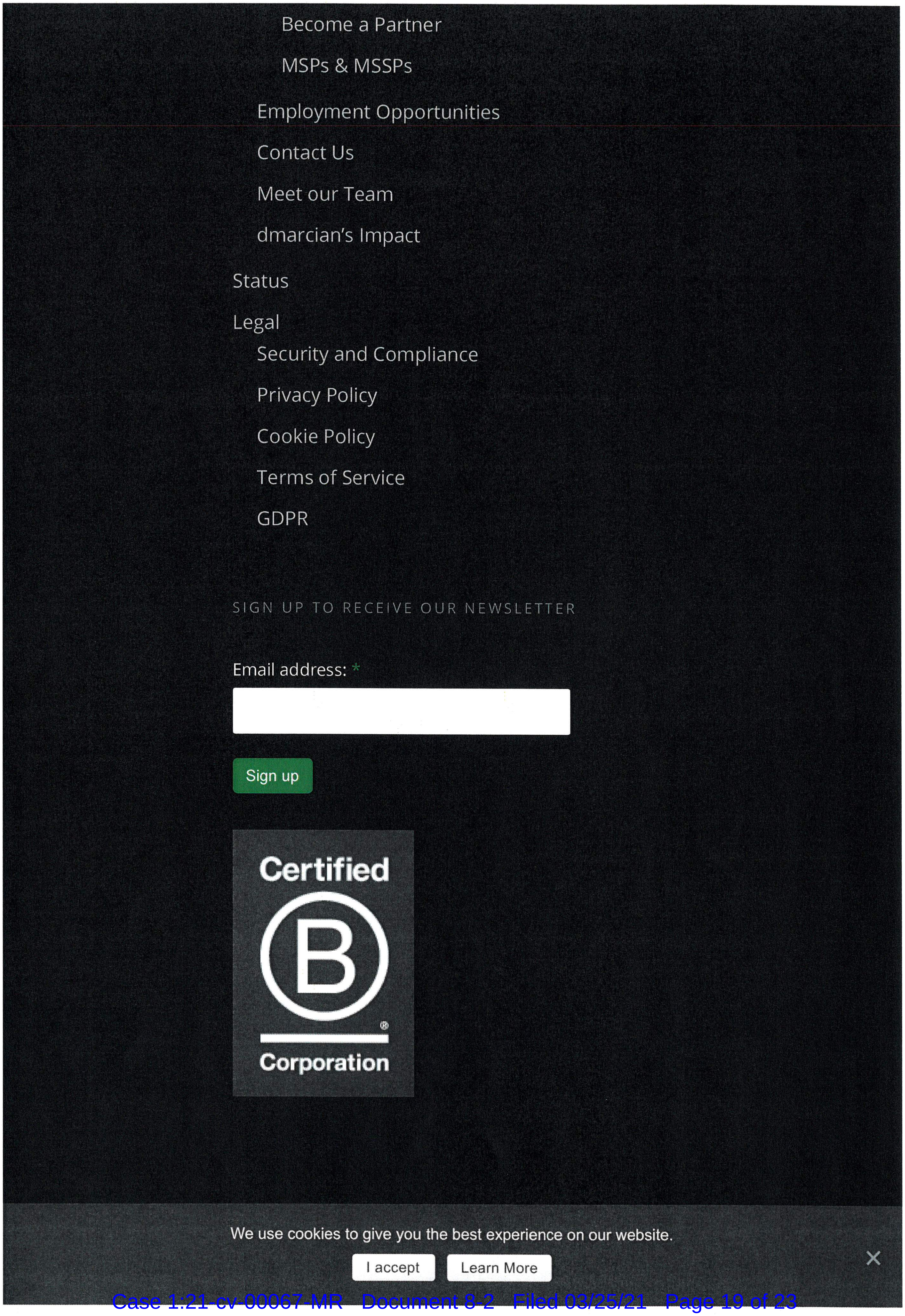
I accept

Learn More

×



We use cookies to give you the best experience on our website.



Become a Partner

MSPs & MSSPs

Employment Opportunities

Contact Us

Meet our Team

dmarcian’s Impact

Status

Legal

Security and Compliance

Privacy Policy

Cookie Policy

Terms of Service

GDPR

SIGN UP TO RECEIVE OUR NEWSLETTER

Email address: *

Sign up

Certified B Corporation

We use cookies to give you the best experience on our website.

AICPA
SOC

© 2021 dmarcian. dmarcian is a registered trademark of dmarcian, Inc.

□ □ □

We use cookies to give you the best experience on our website.

I accept Learn More

dmarcian

Solutions

DMARC SaaS Platform

Allow our application to process and visualize DMARC data in ways that expose authentication gaps (SPF/DKIM) and unauthorized use of your domains.

Recommended for organizations of all sizes and DMARC needs.

LEARN MORE

Deployment Services

Have confidence and expedite your DMARC project timeline by allowing our Deployment Managers to take you through our project-based approach.

Ideal for organizations new to DMARC or ones needing assistance bringing about change.

LEARN MORE

We use cookies to give you the best experience on our website.

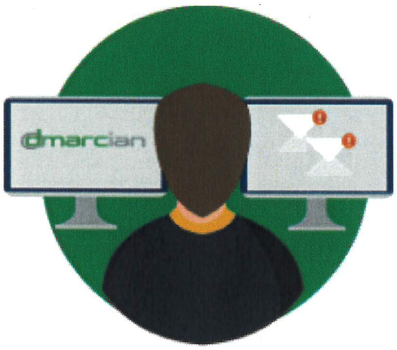
I accept   Learn More

Dedicated Support

Get on-demand support when needs arise. We can help you manage DMARC-related incidents, regular data reviews, ongoing compliance, and embedding DMARC into daily operations.

Best for organizations that need incident-response assurances or intermittent support.

LEARN MORE



142

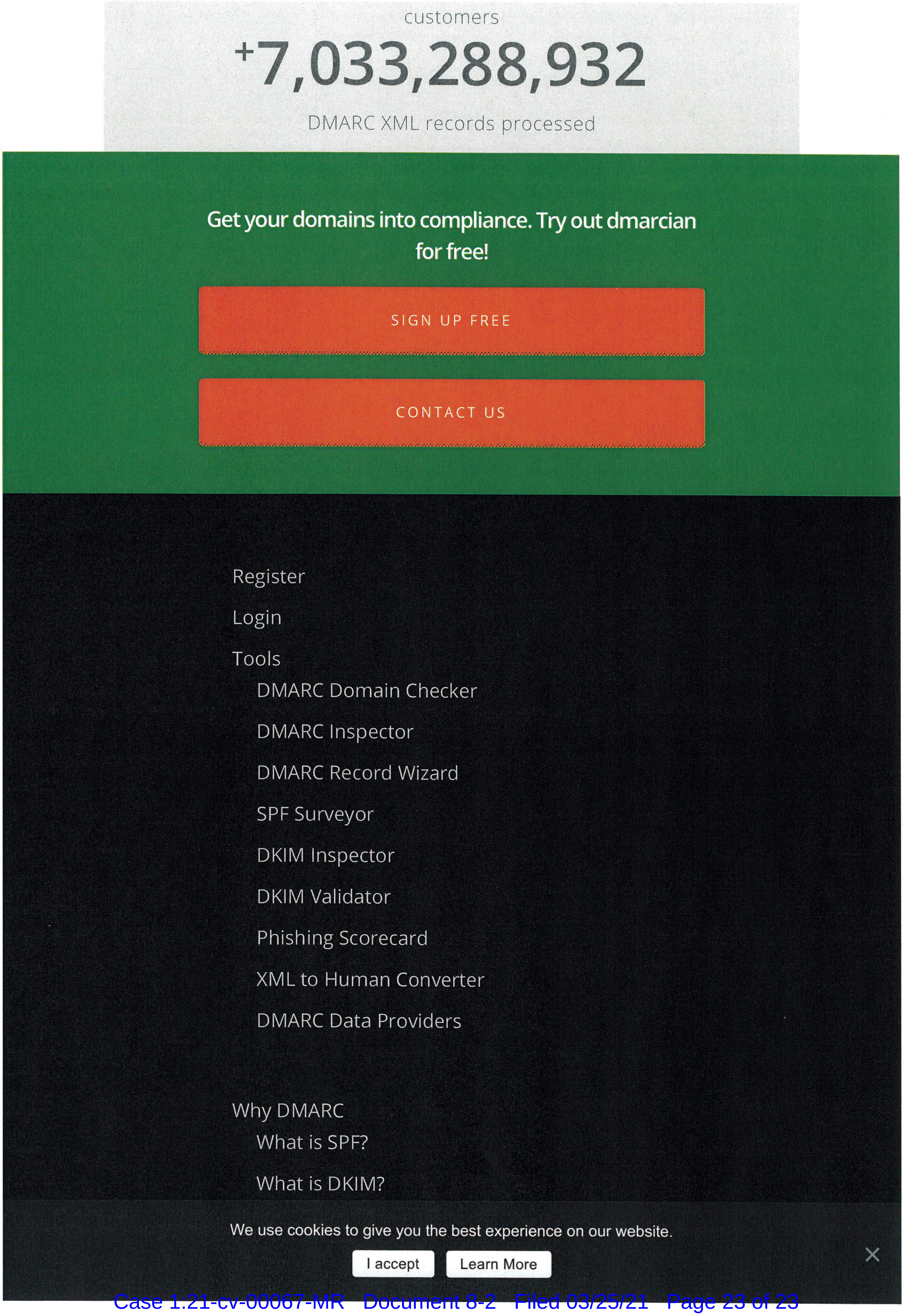
partners

+2,502,448

monitored domains

We use cookies to give you the best experience on our website.

I accept Learn More ×



customers

+7,033,288,932

DMARC XML records processed

Get your domains into compliance. Try out dmarcian for free!

We use cookies to give you the best experience on our website.